PENDING CLAIMS AS AMENDED

Please amend the claims as follows:

Claims 1-11 (Canceled)

12. (Currently Amended) A method for fast generation of a cryptographic key, comprising:

generating a first public key for encrypting a first wireless communication; and

generating, after ~~upon~~ termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key.

13. (Canceled)

14. (Previously Presented) The method of claim 32, further comprising:

using the second public key to encrypt the second wireless communication when it is determined that the second public key has been stored.

15. (Previously Presented) The method of claim 32, further comprising:

generating a third public key to encrypt the second wireless communication when it is determined that the second public key has not been stored.

16. (Currently Amended) A wireless communication device for fast generation of a cryptographic key, comprising:

means for generating a first public key for encrypting a first wireless communication; and

means for generating, after ~~upon~~ termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key.

17. (Canceled)

18. (Previously Presented) The wireless communication device of claim 33, further comprising:

means for using the second public key to encrypt the second wireless communication when it is determined that the second public key has been stored.

19. (Previously Presented) The wireless communication device of claim 33, further comprising:

means for generating a third public key to encrypt the second wireless communication when it is determined that the second public key has not been stored.

20. (Currently Amended) A wireless communication device for fast generation of a cryptographic key, comprising:

a processor for generating a first public key to encrypt a first wireless communication and generating, after ~~upon~~ termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in encrypting the second wireless communication; and

a memory for storing the second public key,

wherein the second public key is independent of the first public key.

21. (Currently Amended) A processor for fast generation of a cryptographic key, said processor being configured to:

generate a first public key for encrypting a first wireless communication; and

generate, upon termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key.

22. (Currently Amended) A computer program product comprising instructions for fast generation of a cryptographic key, wherein the instructions upon execution cause a computer to:

generate a first public key for encrypting a first wireless communication; and

generate, after ~~upon~~ termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key.

23. (Previously Presented) The computer program product of claim 22, wherein the instructions upon execution further cause a computer to:

determine whether the second public key has been stored prior to establishing the second wireless communication.

24. (Previously Presented) The computer program product of claim 23, wherein the instructions upon execution further cause a computer to:

use the second public key to encrypt the second wireless communication when it is determined that the second public key has been stored.

25. (Previously Presented) The computer program product of claim 23, wherein the instructions upon execution further cause a computer to:

generate a third public key to encrypt the second wireless communication when it is determined that the second public key has not been stored.

26. (Previously Presented) The processor of claim 21, wherein said processor is further configured to:

determine whether the second public key has been stored prior to establishing the second wireless communication.

27. (Previously Presented) The processor of claim 26, wherein said processor is further configured to:

use the second public key to encrypt the second wireless communication when it is determined that the second public key has been stored.

28. (Previously Presented) The processor of claim 26, wherein said processor is further configured to:

generate a third public key to encrypt the second wireless communication when it is determined that the second public key has not been stored.

29. (Previously Presented) The wireless communication device of claim 20, wherein the processor determines whether the second public key has been stored prior to establishing the second wireless communication.

30. (Previously Presented) The wireless communication device of claim 29, wherein the processor uses the second public key to encrypt the second wireless communication when it is determined that the second public key has been stored.

31. (Previously Presented) The wireless communication device of claim 29, wherein the processor generates a third public key to encrypt the second wireless communication when it is determined that the second public key has not been stored.

32. (Previously Presented) The method of claim 12, further comprising:

determining whether the second public key has been stored prior to establishing the second wireless communication.

33. (Previously Presented) The wireless communication device of claim 16, further comprising:

means for determining whether the second public key has been stored prior to establishing the second wireless communication.

34. (New) A method for fast generation of a cryptographic key, comprising:

generating a first public key and a corresponding first private key for generating a first shared secret key for encrypting a first wireless communication; and

generating, after termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key and a corresponding second private key for generating a second shared key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key.

35. (New) The method of claim 34, further comprising:

generating a third public key and corresponding third private key for generating the second shared key for encrypting the second wireless communication when it is determined that the second public key has not been stored prior to establishing the second wireless communication.

36. (New) A wireless communication device for fast generation of a cryptographic key, comprising:

means for generating a first public key and a corresponding first private key for generating a first shared secret key for encrypting a first wireless communication; and

means for generating, after termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key and a corresponding second private key for generating a second shared key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key.

37. (New) The wireless communication device of claim 36, further comprising:

means for generating a third public key and corresponding third private key for generating the second shared key for encrypting the second wireless communication when it is determined that the second public key has not been stored prior to establishing the second wireless communication.

38. (New) A wireless communication device for fast generation of a cryptographic key, comprising:

a processor for:

generating a first public key and a corresponding first private key for generating a first shared secret key for encrypting a first wireless communication, and

generating, after termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key and a corresponding second private key for generating a second shared key for use in encrypting the second wireless communication; and

a memory for storing the second public key and the corresponding second key, wherein the second public key is independent of the first public.

39. (New) The wireless communication device of claim 38, wherein the processor generates a third public key and corresponding third private key for generating the second shared key for encrypting the second wireless communication when it is determined that the second public key has not been stored prior to establishing the second wireless communication.

40. (New) A processor for fast generation of a cryptographic key, said processor being configured to:

generate a first public key and a corresponding first private key for generating a first shared secret key for encrypting a first wireless communication; and

generate, after termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key and a corresponding second private key for generating a second shared key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key.

41. (New) The processor of claim 26, wherein said processor is further configured to:

generate a third public key and corresponding third private key for generating the second shared key for encrypting the second wireless communication when it is determined that the second public key has not been stored prior to establishing the second wireless communication.

42. (New) A computer program product comprising instructions for fast generation of a cryptographic key, wherein the instructions upon execution cause a computer to:

generate a first public key and a corresponding first private key for generating a first shared secret key for encrypting a first wireless communication; and

generate, after termination of the first wireless communication and prior to initiation of a second wireless communication, a second public key and a corresponding second private key for generating a second shared key for use in encrypting the second wireless communication, wherein the second public key is independent of the first public key.

43. (New) The computer program product of claim 42, wherein the instructions upon execution further cause a computer to:

generate a third public key and corresponding third private key for generating the second shared key for encrypting the second wireless communication when it is determined that the second public key has not been stored prior to establishing the second wireless communication.